UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND A TRAP & TRACE DEVICE ON E-MAIL ACCOUNT ***************	**Misc. No. 06-11**

MEMORANDUM OPINION

Pending before the Court is the Motion to Review Ruling of Magistrate Judge filed by the United States of America (hereafter referred to as the "Government") on January 19, 2006. For the reasons set forth below, the Court grants the motion in its entirety.

BACKGROUND[1]

This matter involves an ongoing grand jury investigation for which the Government submitted an application requesting a court order authorizing the installation and use of a pen register and trap and trace device on an e-mail account. The Government seeks immediate review of the Magistrate Judge's order staying the application and mandating that the Government submit additional legal briefs addressing several questions, including whether 18 U.S.C. § 3122 authorizes the use of pen register and trap and trace devices on e-mail accounts.[2] To be specific, the Government requests "that this Court vacate the order seeking

---

[1] Because this matter remains under seal the Court omitted any facts that would reveal protected information.

[2] The Government sought review pursuant to Civil Rule 40.7(g) of the Rules of the United States District Court for the District of Columbia (colloquially referred to as the "Local Rules"), which states that "the Chief Judge shall . . . hear and determine requests for review of rulings by magistrate judges in criminal cases not

additional briefing and grant the government's original proposed order authorizing its pen register and trap and trace device application." Id. at 2. Because the Court finds that 18 U.S.C. §§ 3121-3127 unambiguously authorize the use of pen registers and trap and trace devices on e-mail accounts, the Court will grant the Government's motion.

ANALYSIS

Carl Sagan[3] reportedly once observed that "[w]e live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology." Undoubtedly, this observation contains an element of truth that explains, to some extent, why the law is sometimes outpaced by advancing technology. In this case, however, the Court is dealing with a federal law that has, in fact, caught up with the pace of technology -- the question is how far it now reaches. To be specific, the Court is presented with the question of whether 18 U.S.C. §§ 3121-3127 authorize the Government to use pen registers and trap and trace devices on e-mail accounts during the course of criminal investigations.

1. The Scope of 18 U.S.C. §§ 3121-3127

The Court's analysis "begins with the statutory text, and ends there as well if the text is unambiguous." Bedroc Ltd. v. United States, 541 U.S. 176, 183 (2004) (noting that "[t]he preeminent canon of statutory interpretation requires us to 'presume that [the] legislature says in a statute what it means and means in a statute what it says there'"). In this case, the statute at

---

already assigned to a judge of the Court . . . ." The Government argued that "time is of the essence" in this "sensitive" investigation and the Magistrate's Judge's order staying the applications and requesting additional briefing "effectively denied the government's application." Gov't Mot. 9.

[3] Carl Sagan was a respected astronomer, educator and Pulitzer Prize-winning author who gained fame as the host of the Emmy- and Peabody-award winning television show *Cosmos*, which aired on the Public Broadcasting System ("PBS").

issue expressly states that:

> An attorney for the Government may make application for an order . . . authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

18 U.S.C. § 3122(a)(1) (citations omitted). The statute further states that:

> Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

Id. at § 3123(a)(1). Accordingly, so long as an attorney for the Government applies for a "pen register" or "trap and trace device" and the court finds that the attorney certified that the information obtained using the devices is relevant to an ongoing criminal investigation, the court is mandated to enter an ex parte order authorizing the use of the devices.

The issue the Magistrate Judge struggled with, and that poses concerns in other areas,[4] is the scope of the statute. Specifically with regard to this case, the question is whether a "pen register" or "trap and trace device" may be a process that obtains information about e-mail communications. The Court again turns to the statute as the first resort for clarification about the meaning of these terms. The statute defines "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or

---

[4] Our own court, as well as at least one other, has considered the question of whether a pen register and trap and trace device may be used to obtain cell site information that reveals the location of a cell phone user. See e.g., In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Info., No. 05-508, 2006 U.S. Dist. LEXIS 588 (D.D.C. Jan. 11, 2006); In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

facility from which a wire or electronic communication is transmitted . . . ." 18 U.S.C. § 3127(3). Thus, a pen register may be a "process" that records outgoing signals from an instrument or facility that transmits "electronic communication." Id.

The statute goes on to define "trap and trace device" to mean "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . . ." Id. at § 3127(4). According to this definition, a trap and trace device may be a "process" that is used to capture incoming electronic impulses to identify the source of an "electronic communication," albeit not the contents of that communication. Id.

These definitions make clear that both a pen register and a trap and trace device may be a "process"[5] used to gather information relating to "electronic communication." Id. As for the term "electronic communication," the statute points to the definition found in 18 U.S.C. § 2510. Id. at § 3127(1) (stating that the term "electronic communication" has the meaning "set forth for such term[] in section 2510 of this title"). That statute defines the term "electronic communication" to mean "any transfer of signs, signals, writing, images, sounds, data, or

---

[5] The statute does not define the term "process," so the Court will give that term its ordinary meaning. Asgrow Seed Co. v. Winterboer, 513 U.S. 179, 187 (1995) ("When terms used in a statute are undefined, we give them their ordinary meaning."). The term "process" is generally understood to mean "a series of actions or operations conducing to an end." Merriam-Webster's Collegiate Dict. 929 (10th ed. 1999); see also Webster's Third New Int'l Dict. 1808 (1981) (defining the term "process" to mean "an artificial or voluntary progressively continuing operation that consists of a series of controlled actions or movements systematically directed toward a particular result or end"). Given the breadth of this term, the Court concludes that it covers software and hardware operations used to collect information.

intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12). Given that the statute defines an electronic communication to be any "transfer of signals" of "any nature" by means of virtually any type of transmission system (e.g., wire, electromagnetic, etc.), there can be no doubt it is broad enough to encompass e-mail communications and other similar signals transmitted over the Internet. It therefore follows that pen registers and trap and trace devices may be processes used to gather information about e-mail communications.

Further support for this conclusion is found elsewhere in the statute, namely in the provision requiring law enforcement agencies to maintain records about pen registers and trap and trace devices used "on a packet-switched data network of a provider of electronic communication service to the public." 18 U.S.C. § 3123(a)(3)(A). The Internet is such a "packet-switched data network." See Microsoft Corp. v. Multi-Tech Sys., Inc., 357 F.3d 1340, 1345 n.2 (Fed. Cir. 2004) (stating that "a 'packet-switched network,' such as the Internet, is one in which data packets are relayed through various stations on a network"). Consequently, the statute obviously anticipates that law enforcement agencies will use pen registers and trap and trace devices on the Internet or, for that matter, any such network used by a provider of electronic communication service to the public, which would include a provider of e-mail service.

The statute's history compels the same conclusion. In 2001, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA Patriot Act"), Section 216 of which explicitly amended the authorities relating to pen registers and trap and trace devices provided in 18 U.S.C. §§ 3121-3127 by expanding the definitions of these devices to include "processes" to obtain

information about "electronic communication." USA Patriot Act, Pub. L. No. 107-56, §216, 115 Stat. 272, 288 (2001). Commenting on the very language that was finally enacted in Section 216 of the USA Patriot Act, several members of Congress highlighted the fact that the amendments would bring the state of the law in line with current technology by making pen registers and trap and trace devices applicable to the Internet and -- more to the point -- e-mail.

For example, a section-by-section analysis of the bill that Representative John Conyers included in the record before the final House vote, which contains the same language that was finally enacted by Congress, states that Section 216 "[e]xtends the pen/trap provisions so they apply not just to telephone communications but also to Internet traffic." 147 Cong. Rec. H7197 (daily ed. Oct. 23, 2001) (statement of Rep. Conyers). In addition, Senator Jon Kyl, who is currently Chairman of the United States Senate Judiciary Subcommittee on Terrorism, Technology & Homeland Security, noted that the same language in the Senate version of the bill "would codify current case law that holds that pen/trap orders apply to modern communication technologies such as e-mail and the Internet, in addition to traditional phone lines." 147 Cong. Rec. S11049 (daily ed. Oct. 25, 2001) (statement of Sen. Kyl). The Congressional Research Service also published a legal analysis of the USA Patriot Act that states that the Act "permits pen register and trap and trace orders for electronic communications (e.g., e-mail)." Charles Doyle, Congressional Research Serv., CRS Report for Congress, Order Code RS21203, The USA PATRIOT Act: A Sketch (Apr. 18, 2002).

The plain language of the statute makes clear that pen registers and trap and trace devices may be processes used to obtain information about e-mail communications. The statute's history confirms this interpretation and there is no support for a contrary result. Accordingly, the Court finds that 18 U.S.C. §§ 3121-3127 authorize the Government to use pen registers and trap and

trace devices on e-mail accounts during the course of criminal investigations.

2. Protecting E-Mail Content

Although it is clear that the scope of 18 U.S.C. §§ 3121-3127 encompasses the use of pen registers and trap and trace devices on e-mail accounts, the Government's use of such processes or devices is not without constraint. The statute states:

> A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication.

18 U.S.C. § 3121(c). Thus, the Government must ensure that the process or device used to obtain information about e-mail communications excludes the contents of those communications.

There is some concern that current technology, particularly the use of a software process to obtain the requested information, increases the risk that content will be impermissibly procured and disclosed to the Government. A perhaps oversimplified response to that concern is that the stricture to avoid the contents of e-mail communications should be easy to comply with so long as the pen register and trap and trace processes or devices exclude all information relating to the subject line and body of the communication. The better approach, however, may be to take heed of the fact that "pen registers" and "trap and trace devices" are statutorily defined as processes or devices that are prohibited from collecting "the contents of any communication." 18 U.S.C. § 3127(3)-(4). Consequently, the argument could be made that any process or device that collects the content of an electronic communication is not, in fact, a pen register or trap and trace device but, instead, is an electronic intercepting device as defined in Title III of the

Omnibus Crime Control and Safe Streets Act, codified at 18 U.S.C. §§ 2510-2520.[6] Consequently, the unauthorized use of that process or device would be subject to the penalties set forth in that statute.

In this case the Government's application and proposed order explicitly identify the information the process or device is intended to collect and noticeably omit content from the request. The Government also assures the Court that the service providers subject to the requested order are experienced at complying with such orders and employ processes that siphon the permitted information without extracting prohibited content. Recognizing that the Court must trust in the expertise and experience of these service providers, particularly when they are installing and using their own processes to capture information in compliance with a court order, some caution nevertheless is warranted to make certain the court order clearly identifies what is permitted and, more importantly, what is prohibited so there is no question about the scope of the authorized activities.[7] The Court concludes that the application and court order at issue here

---

[6] That statute prohibits any person from engaging in the unauthorized "intercept" of "any wire, oral, or electronic communication" and prescribes penalties for violations. 18 U.S.C. § 2511(1). The statute goes on to define "intercept" to mean the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. at § 2510(4). The statute also states that "no part of the contents of such communication and no evidence derived therefrom may be received in evidence . . . if the disclosure of that information would be in violation of this chapter." Id. at § 2515.

[7] See, for example, In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap, 396 F. Supp. 2d 45 (D. Mass. 2005), in which the district court took a more stringent approach by stating that an order authorizing the use of a pen register and trap and trace device should list exactly what may not be disclosed. 396 F. Supp. 2d at 49. The court in that case also included a provision in its order placing the service providers on notice that they may be held in contempt of court for violating the order by disclosing unauthorized content. Id.

satisfy these concerns and clearly avoid e-mail content.

CONCLUSION

Having determined that 18 U.S.C. §§ 3121-3127 unambiguously authorize the Government to use pen registers and trap and trace devices on e-mail accounts during the course of criminal investigations, and that both the Government's application and the Court's order afford sufficient assurances that the contents of e-mail communications will be protected, the Court will grant the Government's motion and issue the order authorizing the requested pen register and trap and trace device to be installed and used on an e-mail account.

February 2, 2006

/s/
Thomas F. Hogan
Chief Judge

This Court is of the view that an order explicitly identifying the permissible information to be captured by the pen register and trap and trace process or device (e.g., the originating IP address, originating header information, return header information, inbound packet payload and outbound packet payload, and the date and time of the communications) -- versus simply copying and pasting the language from the statute allowing "dialing, routing, addressing and signaling information" -- as well as an admonition making clear that the content of e-mail is prohibited, serves the same purpose.